UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/741,406	12/19/2000	James W. Edwards	10559/295001/P9306	6308

20985 . 7590 02/28/2006

FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER
REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/741,406	**Applicant(s)** EDWARDS ET AL.
	Examiner Christopher A. Revak	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 November 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-12,14-26,28 and 30-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-12,14-26,28, and 30-39* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 December 2000* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 7, 2005 has been entered.

Response to Arguments

2. Applicant's arguments filed November 7, 2005, with respect to the rejection of claims 1-3,5-12,14-26, and 28 under 35 USC 103(a) as being unpatentable over Gilbrech in view of the applicant's admitted prior art have been fully considered and are persuasive. The applicant's arguments are persuasive in that the applicant's specification is not admitted prior art as the examiner has indicated. Therefore, the rejection has been withdrawn. However, upon further consideration, a new grounds of rejection is made in view of Schutte et al, U.S. Patent 6,178,455.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the

> art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claim 1-3,5-12 and 14-39 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claims contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Based on the applicant's arguments, the examiner cannot find support in the applicant's disclosure for the claim language of "the agent component is configured for a dynamically assigned address".

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-3,5-12,14-26,28, and 30-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gilbrech et al, U.S. Patent 6,173,399 in view of Schutte et al, U.S. Patent 6,178,455.

As per claim 1, it is disclosed by Gilbrech et al of a method comprising sending a packet originating from a source (device) across the Internet (public network) to a receiving VPN Unit (agent component) to establish a connection between the source (device) and a LAN (private network)(col. 6, lines 38-41; col. 8, lines 29-55; and as shown in Figures 2 & 5). A connection is established between a router (server component) and a VPN Unit (agent component) since communications are necessary in order for the two to communicate (as shown in Figure 2) and this connection remains active as long as the devices maintain communications with one another unless if that connection is terminated by any or all of the devices. The router (server component) is configured to connect to the VPN Unit (agent component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). It is determined if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (first component) and is forwarded to a VPN Unit (agent component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). The router (server component) creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (agent component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5) wherein the router (server component) receive transmitted messages and forward them to their correct destination, namely the LAN (private network) in light of the teachings of Gilbrech et al (as shown in Figures 2 & 5). The router (server component) is configured to connect to the VPN Unit (agent component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). The router (server component) is configured with a persistent address (col. 8, lines 29-31). The teachings of Gilbrech et al are silent in disclosing that agent component is configured with a dynamically assigned IP address and of maintaining a persistent connection between the agent and the server. The teachings of Schutte et al disclose of dynamically assigning an IP address for a component that is assigned at the beginning of activity by the component and de-assigned at the end of activity with the host (col. 6, lines 27-38) and this connection is interpreted by the examiner as a persistent connection. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply dynamically assigned addresses that are used for persistent connections in that Schutte et al recites of motivational benefits by disclosing of dynamically assigning IP addresses makes it possible to share a small number of addresses with a larger group of users (col. 6, lines 36-38). It is obvious that the teachings of Gilbrech et al would have been able to incorporate dynamic assignment of IP addresses using persistent connections so that a small number of addresses can be used by a larger group of users as is taught by Schutte et al.

As per claims 2 and 11, Gilbrech et al discloses of forwarding a request initiated by a router (second/server component) and is forwarded to a VPN Unit (first/agent component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). The examiner is interpreting the connection between the source (device), VPN Unit (first/agent component), router (second/server component), and device(s) on the LAN (private network) to remain active as long as the devices maintain communications with one another and that the connection is temporary until terminated.

As per claims 3 and 12, Gilbrech et al discloses of determining if the communications from the device conform with authentication rules to connect with the LAN and if so forwarding a request initiated by a router (second/server component) and is forwarded to a VPN Unit (first/agent component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). If the request is not from a recognized member of the VPN group, the packets are discarded (denying the device access)(col. 2, lines 57-67 & col. 8, lines 12-27).

As per claims 5,6,14,15,25, and 26, it is disclosed by Gilbrech et al of a method comprising sending a packet originating from a source (device) across the Internet (public network) to a receiving VPN Unit (first/agent component) to establish a connection between the source (device) and a LAN (private network)(col. 6, lines 38-41; col. 8, lines 29-55; and as shown in Figures 2 & 5). The router (second/server component) is configured to connect to the VPN Unit (first/agent component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). It is determined if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (second/server component) and is forwarded to a VPN Unit (first/agent component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). The router (second/server component) creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (first/agent component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). The examiner is interpreting the connection between the source (device), VPN Unit (first/agent component), and router (second/server component) to remain active as long as the devices maintain communications with one another unless if that connection is terminated by any or all of the devices.

As per claims 7 and 16, Gilbrech et al discloses of determining if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (second/server component) and is forwarded to a VPN Unit (first/agent component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). The examiner is interpreting the authentication rules to include a password since passwords are generally used for authentication.

As per claims 8, 17, and 23, it is recited by the teachings of Gilbrech et al that the public network includes the Internet (col. 2, lines 43-46).

As per claims 9 and 18, Gilbrech et al teaches of determining if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (second/server component) and is forwarded to a VPN Unit (agent/first component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). It is interpreted by the examiner that the VPN Unit (first/agent component) and router (second/server component) are proxy servers since it is disclosed in the applicant's specification "Proxy servers can monitor and intercept any and all requests being sent to and/or received from the private network and/or the Internet. The proxying components can also provide client-to-private-network encryption" as is recited on page 7, lines 13-17. Gilbrech discloses of performing encryption services on the packets and shows how both the VPN Unit (first/agent network component) and router (second/server component) intercept communications since that is the only path into the LAN (private network)(col. 8, lines 19-26 & as shown in Figure 2).

As per claim 10, it is disclosed by Gilbrech et al of a techniques (machine readable instructions stored on an article) for sending a packet originating from a source (device) across the Internet (public network) to a receiving VPN Unit (first component) to establish a connection between the source (device) and a LAN (private network)(col. 6, lines 38-41; col. 8, lines 29-55; and as shown in Figures 2 & 5). The router (second component) is configured to connect to the VPN Unit (first component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). It is determined if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (second component) and is forwarded to a VPN Unit (first component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). The router (second component) creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (first component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5) and the router (second component) receives transmitted messages and forward them to their correct destination, namely the LAN (private network) in light of the teachings of Gilbrech et al (as shown in Figures 2 & 5). The router (second component) is configured to connect to the VPN Unit (first component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). The teachings of Gilbrech et al are silent in disclosing that the first component is configured with a dynamically assigned IP address. The teachings of Gilbrech et al are silent in disclosing that agent component is configured with a dynamically assigned IP address and of maintaining a persistent connection between the agent and the server. The teachings of Schutte et al disclose of dynamically assigning an IP address for a component that is assigned at the beginning of activity by the component and de-assigned at the end of activity with the host (col. 6, lines 27-38) and this connection is interpreted by the examiner as a persistent connection. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply dynamically assigned addresses that are used for persistent connections in that Schutte et al recites of motivational benefits by disclosing of dynamically assigning IP addresses makes it possible to share a small number of addresses with a larger group of users (col. 6, lines 36-38). It is obvious that the teachings of Gilbrech et al would have been able to incorporate dynamic assignment of IP addresses using persistent connections so that a small number of addresses can be used by a larger group of users as is taught by Schutte et al.

As per claims 19 and 36, it is disclosed by Gilbrech et al of a system for sending a packet originating from a source (device) across the Internet (public network) to a receiving VPN Unit (agent component) to establish a connection between the source (device) and a LAN (private network)(col. 6, lines 38-41; col. 8, lines 29-55; and as shown in Figures 2 & 5). The VPN Unit (server component) establishes the connection with the destination (col. 2, lines 57-67 & col. 8, lines 17-26). The request is then forwarded from the VPN Unit (agent component) to the router (server component)(col. 8, lines 52-55 & as shown in Figures 2 & 5). The router (server component) creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (agent component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5) and router (server component) receive transmitted messages and forward them to their correct destination, namely the LAN (private network) in light of the teachings of Gilbrech et al (as shown in Figures 2 & 5). The router (server component) is configured to connect to the VPN Unit (server component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). The teachings of Gilbrech et al are silent in disclosing that agent component is configured with a dynamically assigned IP address. The teachings of Gilbrech et al are silent in disclosing that agent component is configured with a dynamically assigned IP address and of maintaining a persistent connection between the agent and the server. The teachings of Schutte et al disclose of dynamically assigning an IP address for a component that is assigned at the beginning of activity by the component and de-assigned at the end of activity with the host (col. 6, lines 27-38) and this connection is interpreted by the examiner as a persistent connection. It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply dynamically assigned addresses that are used for persistent connections in that Schutte et al recites of motivational benefits by disclosing of dynamically assigning IP addresses makes it possible to share a small number of addresses with a larger group of users (col. 6, lines 36-38). It is obvious that the teachings of Gilbrech et al would have been able to incorporate dynamic assignment of IP addresses using persistent connections so that a small number of addresses can be used by a larger group of users as is taught by Schutte et al.

As per claim 20, Gilbrech et al discloses of a router (server component) that creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (agent component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5) and router (server component) receives transmitted messages and forward them to their correct destination, namely the any devices within the LAN (private network) as is taught by Gilbrech et al (as shown in Figures 2 & 5).

As per claims 20 and 21, Gilbrech et al teaches of forwarding a request from the VPN Unit (agent component) to the router (server component)(col. 8, lines 52-55 & as shown in Figures 2 & 5). The router (server component) creates and establishes the connection (by providing access) between the LAN (private network) and source (device) via the VPN Unit (agent component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). Figure 2 shows multiple devices connected to the LAN (private network).

As per claim 22, it is disclosed by Gilbrech et al that communications are extensible to support any protocol used by the Internet (public network) and the LAN (private network)(col. 5, lines 57-61 & col. 6, lines 5-22). It is interpreted by the examiner that the VPN Unit (agent component) and router (server component) handle the different protocols since they are connected across the Internet (public network) and LAN (private network)(as shown in Figures 2 & 5).

As per claim 24, Gilbrech et al teaches of determining if the communications from the device conform to authentication rules to connect with the LAN and if so, the VPN Unit (agent component) establishes the connection with the destination (col. 2, lines 57-67 & col. 8, lines 17-26).

As per claim 28, it is shown in Figure 2 of Gilbrech et al the routers (server components) are implemented inside the LANs (private networks).

As per claim 30, Gilbrech et al discloses of establishing a connection between the device at the public network and the server after establishing the connection from the agent component to the server (col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). The teachings of Schutte et al are relied upon for disclosing of a persistent connection, please refer above for the motivational benefits as taught by Schutte et al.

As per claim 31, it is taught by Gilbrech et al establishing a connection between the private network and the agent before the establishing of the connection from the agent component to the server (col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). The teachings of Schutte et al are relied upon for disclosing of a persistent connection, please refer above for the motivational benefits as taught by Schutte et al.

As per claims 32 and 35, it is disclosed by Gilbrech et al that the request from the device at the public network travels from the server to the agent prior to reaching the private network (col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5).

As per claim 33, Gilbrech et al teaches of establishing a connection between the device at the public network and the first network component after the establishing of the connection from the second network component to the first network component (col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). The teachings of Schutte et al are relied upon for disclosing of a persistent connection, please refer above for the motivational benefits as taught by Schutte et al.

As per claim 34, it is disclosed by Gilbrech et al of establishing a connection between the private network and the second network component before establishing the connection form the second network component to the first network component (col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). The teachings of Schutte et al are relied upon for disclosing of a persistent connection, please refer above for the motivational benefits as taught by Schutte et al.

As per claims 37 and 38, Gilbrech et al teaches that the agent/server component is implemented within a residential gateway (col. 6, lines 17-22).

As per claim 39, Gilbrech et al discloses that the private network comprises a secured network (col. 6, lines 56-58).

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The cited teachings of Hrastar et al, Merrill et al, Schutte et al, and Bowcutt et al discloses of dynamically assigning IP addresses to components at the beginning of activity by the component and de-assigning at the end of activity.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
Primary Examiner
AU 2131
2/20/06

CR
February 20, 2006